LINK-16 JOINT KEY MANAGEMENT PLAN

JOINT STAFF
WASHINGTON, D.C. 20318

(INTENTIONALLY BLANK)

CHAIRMAN OF THE JOINT CHIEFS OF STAFF MANUAL

J6 Draft CJCSM 6520.01
DISTRIBUTION: A, B, C, J and S 1 April 2002

LINK-16 JOINT KEY MANAGEMENT PLAN

References:

a. CJCSM 6120.01B, March 1, 2000, "Joint Multi-Tactical Digital Information Link Operating Procedures."

b. NAG-45A, August 2001, “Operational Security Doctrine for Joint Tactical Information Distribution System (JTIDS)”

c. NAG-64B, August 2001, “Operational Security Doctrine for Multifunctional Information Distribution System (MIDS)”

d. MCM-109-91, June 17, 1991, "Joint Service Key Management Plan for Joint Tactical Information Distribution System."

1. Purpose. This manual outlines procedures for production, distribution, and use of Link-16 communications security (COMSEC) keying material (KEYMAT). The Joint Multi-Tactical Data Link Operating Procedures manual (reference a) provides further guidance regarding operational management of Link-16 and other tactical data links. References b and c contain NSA Security Doctrine associated with Link-16 devices.

2. Cancellation. The Joint Service Key Management Plan for the Joint Tactical Information Distribution System (reference d) is cancelled.

3. Applicability. This manual provides guidance to Services, Combatant Commanders, Unified Commanders and DOD Agencies involved in the production, distribution, or use of Link-16 KEYMAT.

4. Procedures. This manual documents current key management procedures and procedures applicable to the Electronic Key Management System (EKMS).

5. Additional Copies of Manuals. Joint Staff directorates may obtain a limited number of additional copies of this manual from the Records Management and Automation Support Branch, Room 2B917. Combatant Commands, Services, Defense agencies and all other holders are authorized to reproduce, print, and stock copies to meet internal distribution requirements.

6. Summary. This document establishes procedures to be used by Services, Combatant Commanders and Defense agencies in the production, distribution and management of Link-16 COMSEC material under the current system and EKMS.

7. Releasability. This manual is approved for limited release. DOD components (to include Combatant Commands) and other Federal agencies may obtain copies of this manual through controlled Internet access only (limited to .mil and .gov users) from the CJCS Directives Home Page--http://www.dtic.mil/doctrine. Joint Staff activities may access or obtain copies of this manual from the Joint Staff Local Area Network.

8. Effective Date. This manual is effective upon receipt.

Enclosures:
A - Link-16 Joint Key Management Plan
B - Contact List
GL - Glossary

Draft CJCSM 6520.01
1 April 2002

DISTRIBUTION

Distribution A, B, C, and J plus the following:

Addressee	Number Copies
Office of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence	2
Office of the Undersecretary of Defense for Acquisition, Technology and Logistics	2
Office of the Secretary of Defense Chief Information Officer	1
Office of the Secretary of Defense for Production and Logistics	1
National Defense University	1
Joint Forces Staff College	1
Air Combat Command/Aerospace Command, Control, Intelligence, Surveillance and Reconnaissance Center	1
Air Force Doctrine Center	1
Commander Forces Command	1
Commander Forces Command, Joint Interoperability Division	1
Defense Information Systems Agency Joint Interoperability Engineering Organization	1
Defense Information Systems Agency Joint Interoperability Test Command	1
Joint Doctrine Center	1
Joint Spectrum Center	1
Industrial College of the Armed Forces	1
Joint Command and Control Warfare Center	1
Joint Warfighting Center	1
Military Communications - Electronics Board	1
National Defense University	1
National War College	1
US Forces Japan	5
US Forces Korea	5
Naval Center for Tactical Systems Interoperability	1
US Army Communications and Electronics Command	1
US Army Missile Command	1
USMC Systems Command	1
USMC Combat Development Center	1

USMC Tactical Systems Support Agency	1
Ballistic Missile Defense Organization	1

Draft CJCSM 6520.01
1 April 2002

LIST OF EFFECTIVE PAGES

The following is a list of effective pages for CJCSM 6520.01. Use this list to verify the currency and completeness of the document. An "O" indicates a page in the original document.

PAGE	CHANGE
1 thru 3	O
i thru vi	O
A-1 thru A-12	O
A-A-1 thru A-A-6	O
A-B-1 thru A-B-2	O
A-C-1 thru A-C-4	O
A-D-1 thru A-D-4	O
B-1 thru B-6	O
B-A-1	O
C-1	O
D-1 thru D-8	O

(INTENTIONALLY BLANK)

Draft CJCSM 6520.01
1 April 2002

RECORD OF CHANGES

Change No.	Date of Change	Date Entered	Name of Person Entering Change

(INTENTIONALLY BLANK)

TABLE OF CONTENTS

Page

CHAPTER ONE

GENERAL INFORMATION

1.1 Background. Link-16 is the DoD and North Atlantic Treaty Organization primary tactical data link for Service and Defense agency command and control, intelligence, and, in some cases, weapons systems applications. It is a secure, jam-resistant data link using the Joint Tactical Information Distribution System (JTIDS - AN/URC-107 Series) and Multi-functional Information Distribution System (MIDS) Low Volume Terminal (LVT) (AN/USQ-140 Series) family of terminal sets. Link-16 supports functional mission areas including joint theater air and missile defense, attack operations, counter-air, interdiction, suppression of enemy air defenses, close air support and time critical targeting prosecution. Link-16 networks may include allied or coalition forces and are protected by communications security (COMSEC) equipment and keying material (KEYMAT). Link-16 KEYMAT will be generated and distributed by the Electronic Key Management System (EKMS), described in chapter three. Prior to full EKMS implementation, the key management process described in chapter two remains effective.

1.2 System Description. Link-16 uses a uniquely defined waveform and frequency range (969-1206 MHz) for digital voice and packet message communication. Terminals communicate using the Link-16 message standard format defined in MIL-STD 6016A and a time division multiple access (TDMA) architecture with participant transmissions assigned to specific time slots. Link-16 typically functions as a line of sight system capable of operating in the normal mode of operations at a range of 300 nautical miles or an extended mode at a range of 500 nautical miles. This range can be further extended through the use of relay platforms.

1.2.1 Hardware. Table 1-1 describes Link-16 terminals and associated platforms.

1.2.2 Transmission Characteristics.

1.2.2.1 Time Division Multiple Access (TDMA). The TDMA transmission structure decomposes data into message sets transmitted during pre-planned intervals (time slots). Each participating terminal is allocated time slots to transmit, receive, or relay data. Within each time slot, radio terminal transmission/reception “hops” among 51 discrete frequencies to improve jam resistance. This pseudo-random frequency hopping sequence is determined

Terminal	Size	Power	Users	Platforms
JTIDS Class 1	6 cu ft 310 lbs	200/1000 Watts	Air Force	ASIT
JTIDS Class 2	1.6 cu ft 130 lbs	200 Watts	Air Force Navy	JSTARS MCE ABCCC F-15 F-14D
JTIDS Class 2H	3.25 cu ft 220 lbs	200/1000 Watts	Air Force Navy Marine Corps	AWACS AEGIS CG/DDG CVN/LHD/LCC E-2C TAOM TAOC
JTIDS Class 2M	1.3 cu ft 89 lbs	40/200 Watts	Army	PATRIOT JTAGS ADTOC SHORAD THAAD
MIDS LVT -1	0.61 cu ft 65 lbs	30/200/1000 Watts	Navy Air Force	F/A-18 NHPS F-16
MIDS LVT-2	1.35 cu ft 86.9 lbs	30/200 Watts	Army	PATRIOT THAAD MEADS
MIDS LVT-3 (FDL)	0.61 cu ft 65 lbs	40 Watts	Air Force	F-15
Front End System (FES)	0.88 cu ft 45 lbs	Receive Only	All Services	Support systems

Table 1-1 - Link-16 Terminals, Users and Associated Platforms

by the transmission key. Further information regarding the Link-16 waveform may be found in the MIDS System Segment Specification.

1.2.2.2 Time Slot. A time slot is a standard interval (7.8125 msec) assigned to individual Link-16 participating units for message transmission. With the exception of voice, round trip timing (RTT) and free text, data transmitted within a time slot is composed of three, six or twelve 70-bit words, depending on the packing structure used. Network design establishes the assignment of transmit and receive time slots to each participating platform.

1.2.2.3 Network Participation Groups (NPGs). NPGs are the basic Link-16 communication "circuits." Each Link-16 network design assigns time slots within NPGs based on the type of information being exchanged. NPGs include net entry, precise participant location and identification (PPLI), round trip timing (RTT), net management, mission management, surveillance, and voice, among others. Messages produced by host combat systems are routed for transmission to specific, but arbitrary, NPGs. Since terminals provide NPG filtering and selection, message assignment by NPG may be used for partitioned security and selective filtering.

1.2.3 Network Management.

1.2.3.1 Network Selection. Link-16 networks are selected from the JTIDS Network Library (JNL) based on the theater datalink architecture or operational and training requirements. Operational architectures normally require use of a US joint or allied operational key. Training architectures may require the use of specialized key.

1.2.3.2 Network Deconfliction. A Link-16 network is a group of participants in time synchronization and exchanging information. Planning is required to ensure different networks (encompassing different participants and/or purposes) do not cause mutual interference. There are three ways to ensure successful independent network operations: geographic separation such that synchronization cannot be achieved between two different networks; different key (cryptographic differentiation); or network time offset. When independent operations are sufficiently close that inadvertent synchronization between networks is possible, use of different key (i.e., a different short title) is the preferred method for resolving independent networks. Network time offset may be used for training operations or when the use of different key is not operationally feasible. Time offsets shall be managed to ensure that no single terminal reuses key.

1.3 Security. Link-16 circuits may be used to transmit information up to and including SECRET. Link-16 has been evaluated and is approved by the

National Security Agency Director (DIRNSA) for operation in the SECRET HIGH security mode if all network participants are cleared for SECRET and have access approval for all information in the Link-16 net. NSA has also assessed Link-16 for the exchange of compartmented and special access information. Although NSA cannot currently certify Link-16 for operation in compartmented mode, segregation can be accomplished by using a separate key for a specific NPG. Because of these information segregation features, a particular Designated Accrediting Authority or Certifying Authority can, after their own risk assessment, authorize Link-16 for exchange of compartmented or special access information (up to TOP SECRET HIGH) associated with their program. The full cryptographic and information segregation feature of Link-16 should be used. Each program must evaluate alternatives and specify procedures (e.g. special key, special messages or additional encryption). All personnel authorized uncontrolled access to Link-16 terminal areas must be cleared at least to the classification level of the Link-16 data being exchanged. Link-16 terminals currently use a THORNTON-based Secure Data Unit (SDU) making them cryptographically compatible. The SDU provides both Transmission Security (TSEC) and Message Security (MSEC).

1.3.1 Transmission Security (TSEC). Each Link-16 terminal can operate on any one of 127 different nets, each net defined by a distinct pseudo-random frequency-hopping pattern, increasing resistance to jamming and exploitation. TSEC key assignment is one of the Link-16 network initialization parameters and, together with the time slot number, determines the hopping sequence for each net and provides symbol interleaving, pulse modulation encryption, carrier frequency hopping, and message start jitter. TSEC key is also used to transmit connectivity maintenance messages such as Precise Participant Location and Identification (PPLI).

1.3.2 Message Security (MSEC). Link-16 messages are transmitted via data blocks and encrypted using an MSEC key assigned by the Link-16 network initialization parameters. Traffic Encryption Keys (TEKs) provide Link-16 MSEC.

1.4 Keying Material (KEYMAT). A standard 128-bit TEK provides both TSEC and MSEC. A standard 256-bit Key Encryption Key (KEK) or RUTTER (KOK-13) KEK encrypts and decrypts TEK to decrease risk of exploitation during distribution, issue and loading.

1.4.1 Traffic Encryption Key (TEK). TEK is the basic key for encrypting operational message traffic. TEK provides TSEC and MSEC.

1.4.2 Key Encryption Key (KEK). A long-term goal of EKMS is to minimize human access to KEYMAT. One strategy used to protect KEYMAT from

exploitation is encryption using KEK. The four types of KEKs (yielding four corresponding types of encrypted KEYMAT) are listed in Table 1-2.

KEK	Protected Material	Protected Path	Specific Protected Material	KEK Account/Load	KEK Production Location
OTAR KEK	Individual keys	Over the air from system controller Link-16 terminal to remote Link-16 terminal	Link-16 TEKs, OTAR KEKs	At KOK-13 and Location 5 of Link-16 SDU	In the KOK-13 or Tier 2
ECU KEK	Individual keys	From Tier 2 through Tier 3 DTD to ECU	Link-16 TEKs, ECU KEKs[1], OTAR KEKs	At Tier 2 and ECU	At Tier 1 or Tier 2
TrKEK	Individual keys	From Tier 2 to Tier 3 DTD	Link-16 TEKs, ECU KEKs, OTAR KEKs	At Tier 2 and DTD	At Tier 2
EKMS KEK	Bulk keys sets	Between Tier 0, Tier 1, and Tier 2	See EKMS Doctrine	At Tier 0, Tier 1 and Tier 2	At Tier 0, Tier 1, and Tier 2

[1] Although encryption of ECU KEKs in ECU KEKs is technically possible, procedures for accomplishing this have not been developed.

Table 1-2 - KEK Types

1.4.2.1 Over-the-Air Rekey (OTAR) KEK. OTAR KEK (sometimes referred to as the “unique”) is loaded in the SDU and used to encrypt and decrypt a “re-key phrase.” This re-key phrase is transmitted to the Link-16 terminal and processed by the SDU when conducting over-the-air re-keying and will be subsequently referred to in this document as OTAR Encrypted Key. Unlike other Link-16 keys, OTAR Encrypted Keys are always received by the SDU through the terminal interface rather than the fill port interface.

1.4.2.2 End Cryptographic Unit (ECU) KEK. ECU KEK is installed in the KGV-8B or CDH (COMCSEC/TSEC Integrated Circuit (CTIC) Data Standard 101 Hybrid) end cryptographic unit (ECU). The Encrypted key obtained from the ECU KEK is an ECU Encrypted Key. ECU Encrypted Keys are received through the fill port. A proposed MIDS enhancement would allow ECU Encrypted keys to be received by the SDU from the terminal interface.

1.4.2.3 Transfer KEK (TrKEK). EKMS utilizes encrypted key distribution from the Tier 2 EKMS Manager level to the Tier 3 "user" (key loader) level. Tier 2 encrypts keys for the user in a Transfer KEK (TrKEK). This KEK installed in

the Tier 3 AN/CYZ-10 Data Transfer Device (DTD). The encrypted keys protected by this TrKEK are referred to in this document as DTD Encrypted Keys. The DTD uses the TrKEK to decrypt the DTD Encrypted Keys prior to loading into an SDU. Although there are additional KEK and encrypted storage keys internal to EKMS sometimes also referred to as TrKEK, they will not be addressed here. For the purposes of this document, TrKEK describes KEKs used to encrypt individual keys from Tier 2 to the DTD.

1.4.2.4 Electronic Key Management System (EKMS) KEK. EKMS KEK is used for data and key bulk encryption and are used to protect key transferred between EKMS Tier 0, Tier 1, and Tier 2.

1.4.3 Key Availability. Link-16 COMSEC is established through use of either the Common Variable Mode (CVM), in which a single TEK is used to provide both TSEC and MSEC, or the Partitioned Variable Mode (PVM), in which one TEK is used for TSEC and a different TEK is used for MSEC. Coordinated joint operations require that different platforms use the same TEK short titles and coordinated network from the JNL to supply the initialization parameters to the platforms. Link-16 is structured to support multiple CRYPTONETs using different TEKs (i.e., it can use more than one short title at a time), and the system is capable of smoothly operating on four CRYPTONETs simultaneously. Although no maximum size limit is prescribed for Link-16 TEK CRYPTONETs, they should be as small as operationally feasible. The same TEK short title shall not be used worldwide to minimize the risk of global compromise. To facilitate compliance with this requirement, a worldwide key is available for emergency and contingency operations, and four TEKs are available for each regional Combatant Command. Each command may use its collection of short titles as operationally required. Chapter four describes procedures followed by Combatant Commands when ordering short titles. EKMS generates and distributes keys that are then globally pre-positioned. Availability of required keys at pre-positioned sites and pre-assigned EKMS Tier 2 servicing facilities enables rapid key distribution. Combatant Commands should include Link-16 key distribution in Operational and Contingency Plan development.

1.4.4 Key types. Since Link-16 key is available in either unencrypted or encrypted format, appropriate KEKs are generated, distributed and issued along with the encrypted form of any short title at the lowest practical EKMS Tier. ECU Encrypted Keys, both TEK and KEK, shall be used wherever feasible. Encryption of unencrypted keys is the responsibility of the commander at the lowest EKMS Tier 2 distribution element. KEK is used to protect the movement of underlying unencrypted key from the local EKMS account through to the using ECU. It is the responsibility of the command

encrypting a key to manage KEK distribution to the ECU for decryption of the ECU Encrypted Keys.

1.4.4.1 Operational Keys. These keys are used to support operational missions. They are at least SECRET CRYPTO and change each cryptographic period. They are designated either for special global use or for a specific combatant command.

1.4.4.2 Maintenance Keys. These global keys are used to support maintenance and training. They are FOUO or higher (some users may require SECRET keys that do not change for each cryptographic period to conduct security training). Maintenance keys are also used in research, development, test and evaluation.

1.4.4.3 Test Keys. These keys are used to conduct "on the air" testing under operational conditions. They include SECRET keys that change for every cryptographic period (global, but not necessarily pre-positioned) and unclassified cryptographic annual supersession key. Operators should select appropriate key based on classification requirements precipitated by the test. Operational key may also be used for test purposes within the valid cryptographic period for that key.

1.4.5 Operational Key Allocation. Link-16 requires several operational keys.

1.4.5.1 Emergency Contingency Operational Key. One set of joint keys will be maintained for worldwide emergency contingency use. This set will be held by all Link-16 user COMSEC accounts and used only under direction of the Joint Staff to support an emergency in which users from different combatant AORs must arrive in a theater of operations on short notice. The Joint COMSEC Management Office (JCMO) orders short title for Emergency Contingency Operational Key.

1.4.5.2 Joint Theater Key. Used for operations among US commands within a theater of operations. During normal operations a separate set of short titles will be used for each Combatant Command. If units from a supporting Combatant Command are involved, they will obtain key from the supported Commander as part of the normal planning process. Availability of four short titles provides flexibility and the potential for multiple cryptographic networks.

1.4.5.3 Allied Keys. Used for operations within an area of operations that include allied elements. During normal operations a separate set of short titles will be used for each Combatant Command. Units from a supporting Command are involved in operations will obtain keys from the supported Combatant Commander as part of the normal planning process. Allied key distribution may also require NSA to distribute key outside EKMS.

1.4.6 Crypto Period. TEK and ECU KEK are distributed using the Edition/Segment convention.

1.4.6.1 Traffic Encryption Key (TEK). Each TEK edition has a one month cryptographic period, and each TEK segment has a one-day cryptographic period. Except when using time offset to operate independent networks, the TEK cryptographic period begins exactly one minute before 0001 Universal Coordinated Time (UTC) and ends exactly one minute after 2359 UTC. TEK cryptographic period shall not be extended except in cases where the Link-16 terminal has been initialized in the seven-day mode. Explicit coordination and a Joint Service agreement are required to use a seven-day cryptographic period. Although all Link-16 terminals are capable of operating in a seven-day mode, many platform C2 systems are not. If one Link-16 unit in a net uses the seven-day mode, all network participants are required to operate in the seven-day mode.

1.4.6.2 Key Encryption Key (KEK). Each ECU KEK edition has a six month cryptographic period, and each ECU KEK segment has a one month cryptographic period. When Link-16 ECU KEK is generated, the cryptographic period is prescribed to coincide with the TEK it encrypts/decrypts.

1.5 Secure Data Unit (SDU). Link-16 terminals use a THORNTON based Secure Data Unit (SDU) making them cryptographically compatible. The THORNTON family includes various types of SDUs and supporting equipment. The number of keys they may store -- 8 or 64 -- and the COMSEC key loading protocol distinguishes the various SDUs.

1.5.1 SDU Types. SDUs are divided into two major categories based on common functional characteristics.

1.5.1.1 KGV-8(E-2), KGV-8A, KGV-8C and E-GLD. These devices can store and use only TEK and OTAR KEK. Eight random access memory (RAM) locations are available for daily use key storage. These SDUs are keyed via DS-102 protocol and can only receive key in the unencrypted form. An external Keyer Control Panel (KCP) or Load Control Unit (LCU) is required to manually select the desired memory location for the key fill process. All keys stored in RAM are non-extractable and are erased when power is removed from the SDU.

1.5.1.2 KGV-8B and CDH. These devices can be filled with either unencrypted or encrypted TEK in any of eight (or sixty-four for MIDS LVT-2) RAM storage locations. All keys are stored in unencrypted form. Encrypted keys are decrypted by their associated pre-loaded KEK prior to storage in RAM. Nine Electronically Erasable Programmable Read Only Memory (EEPROM) locations are available for KEK storage. Keys stored in EEPROM are also stored in

unencrypted form. All keys stored in either RAM or EEPROM are protected from extraction and exploitation by other means. All keys stored in RAM are erased when power is removed from the SDU. Keys stored in EEPROM can only be erased upon receiving an external command from a DTD. These SDUs are filled via the DS-101 protocol and do not require a KCP. A DTD running the Common Tier 3 DTD User Application Software (CT3 DTD UAS) or the JTIDS DTD Key Management Software (JTIDS DTD KMS) provides the correct DS-101 loading information to set the SDU location into which the key is to be stored.

1.5.2 Characteristics. SDUs are distinguished by the number of keys they may store and the COMSEC key loading protocol — NSA Specification Standard DS-102 Common Fill Device Interface Protocol and NSA Specification Standard DS-101 Data Packet Exchange Protocol. The CDH can be configured to work with either protocol (DS-102 or DS-101), but the only terminal that allows both is the JTIDS Class II PIP using the Common Signal Processor (CSP) card. All other uses of the CDH are set to one protocol or the other in the terminal design. Table 1-3 shows the Link-16 terminal types and their associated SDU.

Terminal	SDU	Key Format/Protocol
Class 1	KGV-8	8 keys / DS-102
Class 2	KGV-8 KGV-8A/C KGV-8B[1]	8 keys / DS-102 8 keys / DS-101
Class 2 PIP	CDH on CSP Card[2]	8 keys / DS-102 or DS-101
Class 2H	KGV-8 KGV-8A/C KGV-8B[1]	8 keys / DS-102 8 keys / DS-101
Class 2M	E-GLD (EMD models only) CDH embedded on CSP Card[2]	8 keys / DS-102 8 keys / DS-101 or DS-102
MIDS LVT(1)	CDH embedded on SMP Card[1]	8 keys / DS-101
MIDS LVT(2)	CDH embedded on SMP Card[1]	64 keys / DS-101
MIDS LVT(3) (FDL)	CDH embedded on SMP Card[1]	8 keys / DS-101
Front End System (FES)	CDH embedded on TCU Card[1]	8 keys /DS-101 or DS-102

Table 1-3 - Link-16 Terminal/SDU Use

[1] The DS-101 ECU, such as the KGV-8B and CDH may be filled with an encrypted ECU Encrypted key which uses an ECU KEK for encryption and decryption. Consequently, there are 9 additional EEPROM key locations for storage of KEKs.

[2] The CSP (CDH) can be installed as either DS-102 or DS-101. There are switches on the card itself to select which protocol will be used.

1.5.2.1 Fill Port. The SDU fill port is designed in accordance with the Interoperability Standards for Electronic Key Management Systems (ISEKMS 308) protocol standard. Keys can be loaded into the E-GLD, KGV-8(E-2), KGV-8A and KGV-8C using the Common Fill Device Interface (CFDI) protocol (commonly referred to as DS-102). Keys can be loaded into the KGV-8B or CDH using the DS-101 Data Packet Exchange Protocol as limited and augmented by NSA Specification 90-2A.

1.5.2.2 Cryptographic Periods. Link-16 KEYMAT cryptographic periods extend from exactly one minute before 0001 UTC to exactly one minute after 2359 UTC.

1.5.2.3 Cryptographic Engine. Link-16 terminals currently use an SDU with a THORNTON based COMSEC/TSEC Integrated Circuit (CTIC) as the primary cryptographic engine. The CTIC encrypts and decrypts messages for each time slot (128 per second). Although the SDU can use the same key for generating the bits used for TSEC as well as for encrypting and decrypting messages (MSEC), a different key may be used for MSEC if desired. There are eight SDU RAM locations that may be used to store keys (sixty-four locations in the MIDS LVT(2)). Normally half the locations are used for the current day and half are reserved for the next day. At exactly one minute after 2359 UTC, the terminal triggers the SDU to switch to the next day's keys and erase previously used keys.

1.5.2.4 Special Capabilities. The terminal can also insert an OTAR Encrypted Key in the SDU at a prescribed time and instruct the SDU to decrypt and store this key into any of its memory locations. An OTAR KEK must have been previously loaded into location 5 and the terminal initialized for OTAR.

1.5.2.5 Automatic Rollover. Unlike systems that require key loading at the change of each cryptographic period (e.g., daily), Link-16 is designed to automatically rollover to a new key at the end of each cryptographic period. Except when using time offset to operate independent networks, Link-16 rollover occurs at the end of the minute defined by 2359 UTC.

1.5.2.6 SDU Location Pairs. Link-16 utilizes its SDU RAM storage locations in pairs (0/1, 2/3, 4/5, etc.). Keys for successive cryptographic periods are loaded into each pair. If the terminal is using a key in SDU RAM location 0, the terminal begins using the key in location 1 at rollover and will erase the key

in location 0. This relieves the system operator from either loading a new key or performing a manual switch. Keys may be loaded for the next succeeding cryptographic period at the operator's convenience. At the end of the next cryptographic period the terminal begins using the key in location 0 (provided a new key has been loaded) and erases the key in location 1. The same procedure applies for pairs 2/3, 4/5, etc. (the 4/5 pair does not roll over if the terminal has been initialized to use OTAR). The Link-16 terminal is required to rollover all the locations in the same way, from even to odd, or odd to even (it will not rollover a 0 to 1 and at the same time a 7 to 6). To keep the Link-16 in continuous operation, it is required that key fill take place daily. It is important that successive key fill take place before the second rollover.

1.6 Key Loading Devices. COMSEC key loading devices include the AN/CYZ-10 DTD, the KYK-13, KYX-15, and the KOI-18. The AN/CYZ-10 DTD, running the CT3 DTD UAS, is the primary EKMS fill device. The AN/CYZ-10 DTD is used to load either the DS-102 or DS-101 protocol SDU and is the only device that can fill the KGV-8B and CDH utilizing the DS-101 protocol. Key is loaded into the AN/CYZ-10 DTD using the EKMS Tier 2 workstation. The Key Distribution Support User Application Software (KDSU), that runs in the EKMS Tier 2 platform, or the Data Management Device (DMD) can provide the necessary calculations and provide the location and mission information to the AN/CYZ-10 DTD for both DS-101 and DS-102 SDUs. The Army plans to use ACES to do these calculations and provide the locations and mission information. Manual entry of this information into the AN/CYZ-10 DTD is also possible. If EKMS cannot provide electronic key and paper keys are necessary, key can be loaded into the AN/CYZ-10 DTD by attaching a KOI-18 and pulling the paper key through the KOI-18 as directed by the CT3 software. The KYK-13 and KYX-15 can be used to fill the KGV-8(E-2), E-GLD, KGV-8A, and KGV-8Cs and are expected to be phased out after the full EKMS implementation. There are currently no plans to phase out the KOI-18.

1.6.1 AN/CYZ-10 DTD Preparation. Prior to loading the SDU, the AN/CYZ-10 DTD UAS is set up for the specific SDU. The AN/CYZ-10 DTD UAS supports Link-16 by providing an automated set of procedures for assistance in loading key. Optimally, the UAS allows the user to press one button on the keypad to initiate key loading. Specific identifying data is associated with each SDU in the form of a Station Identifier (STATION ID) and a Station Bus Address (STATION ADDRESS) for use in single point keying configurations. A personal computer (PC) based UAS provides users with an automated means of gathering, collating, and formatting the data for transfer to the AN/CYZ-10 DTD using either an RS-232 Serial or High-level Data Link Control (HDLC) protocol. The data includes Key Tag, cryptographic period, classification, a unique text identifier (TEXT ID) and effective date information for the required

keys, SDU RAM or EEPROM storage location and a unique terminal/equipment STATION ID. Additionally, data obtained from the OPTASK LINK message is transferred from the PC to the AN/CYZ-10 DTD. Data is transferred from the PC to the AN/CYZ-10 DTD before or during key loading. Provisions are available for manual entry of identifying data directly into the AN/CYZ-10 DTD. Only after the identifying data has been transferred to the AN/CYZ-10 DTD can keys be loaded into the Link-16 SDU. Keys are loaded into a AN/CYZ-10 DTD from a Tier 2 PC, another AN/CYZ-10 DTD or from a KOI-18 tape reader. Electronic key distributed through Over-The-Air Transmission (OTAT) can be received directly by a DTD.

1.6.2 Loading TEK. To support automatic rollover, TEKs must be loaded into the SDU in adjacent pair RAM storage locations. Key management data pre-loaded into the DTD establishes which TEK segment is to be loaded into which SDU RAM location. TEK is loaded into the Link-16 SDU daily. During continuous Link-16 operations during which the terminal is not powered off daily, only the next day TEK should be loaded. If the terminal has been powered off, both the current day and next day TEK must be reloaded. The DTD UAS manages daily key loading. Terminals utilizing the KGV-8B must be loaded with the current and next day's TEK each time key is loaded. CT3 software is designed to do this automatically.

1.6.3 Current Cryptographic Period Designator/Cryptographic Period Designator. The initialization parameter referred to as the Current Cryptographic Period Designator (CCPD) governs and standardizes which locations are in use on a given day. The CCPD is zero on January 1, 1985 and alternates between zero and one for each day thereafter. Within the terminal initialization load parameters, each of the terminal SDU locations has a Cryptographic Period Designator (CPD) associated with it. The terminal will only use the location whose CPD agrees with the CCPD. Even locations have the same CPD and the odd locations have the opposite CPD. It is important that the terminal operator provide the terminal with information required to establish the correct CCPD. Some system installations require the CCPD be entered manually from the operator's console. Other systems may require only that the correct date (day, month, year) be maintained by or entered into the system. A standardized CPD initialization ensure interoperability among universally distributed JNL networks. When loaded into the Link-16 system the same default CPD is set by the initialization data. The current CPD for the network initialization data load must be modified immediately prior to or immediately after KEYMAT loading or re-loading.

1.6.4 Key Loading. To ensure the terminal has the correct CCPD, personnel must ensure keys are loaded into memory locations that match the CPD

assigned by the terminal initialization parameters. The DTD UAS manages this function for DS-101 SDUs. For DS-102 protocol key loading, the user must manually set the appropriate switches on the terminal or KCP to select the appropriate SDU RAM storage location to match the automated assignment being made by the DTD UAS. The appropriate location information is obtained from the applicable OPTASK LINK message and the cryptographic period determination table (Table 1-4). For Link-16 terminals using a DS-102 type SDU, indications for success of a key load are displayed on the KCP or LCU immediately after each key segment is loaded. For DS-101 SDUs, the DTD will display the status of the key load after the load has been completed. The DTD also records this information in the key load status log. This log can be reviewed or reset at the DTD or uploaded to a PC for storage or printing.

Current Crypto Period Designator (CCPD) Table Non-Leap Years							Current Crypto Period Designator (CCPD) Table Leap Years					
1997, 1999, 2002, 2005, 2007, 2010, 2013, 2015			1998, 2001, 2003, 2006, 2009, 2011, 2014, 2017				2000, 2008, 2016			1996, 2004, 2012		
Month	Day is... Odd	Even	Month	Day is... Odd	Even		Month	Day is... Odd	Even	Month	Day is... Odd	Even
JAN	1	0	JAN	0	1		JAN	0	1	JAN	1	0
FEB	0	1	FEB	1	0		FEB	1	0	FEB	0	1
MAR	0	1	MAR	1	0		MAR	0	1	MAR	1	0
APR	1	0	APR	0	1		APR	1	0	APR	0	1
MAY	1	0	MAY	0	1		MAY	1	0	MAY	0	1
JUN	0	1	JUN	1	0		JUN	0	1	JUN	1	0
JUL	0	1	JUL	1	0		JUL	0	1	JUL	1	0
AUG	1	0	AUG	0	1		AUG	1	0	AUG	0	1
SEP	0	1	SEP	1	0		SEP	0	1	SEP	1	0
OCT	0	1	OCT	1	0		OCT	0	1	OCT	1	0
NOV	1	0	NOV	0	1		NOV	1	0	NOV	0	1
DEC	1	0	DEC	0	1		DEC	1	0	DEC	0	1

Table 1-4 - Crypto Period Determination Table

CHAPTER TWO

INTERIM LINK-16 KEY MANAGEMENT

2.1 Current Key Management Procedures. This chapter outlines the interim process by which Link-16 key is currently being managed prior to full EKMS transition.

2.1.1 USN Key Management. USN Link-16 terminals use unencrypted TEKs and KEKs from punched paper tapes and encrypted TEKs on floppy disks. Keys are requested by user COMSEC accounts through the Director COMSEC Material Systems (DCMS), generated by NSA, then shipped to user accounts by the NSA-managed National Distribution Authority (NDA). Encrypted TEKs are loaded into DTDs using JTIDS personal computer UAS. Local COMSEC managers submit key requests through controlling authority. Figure 2-1, depicts the current USN Link-16 key management process.

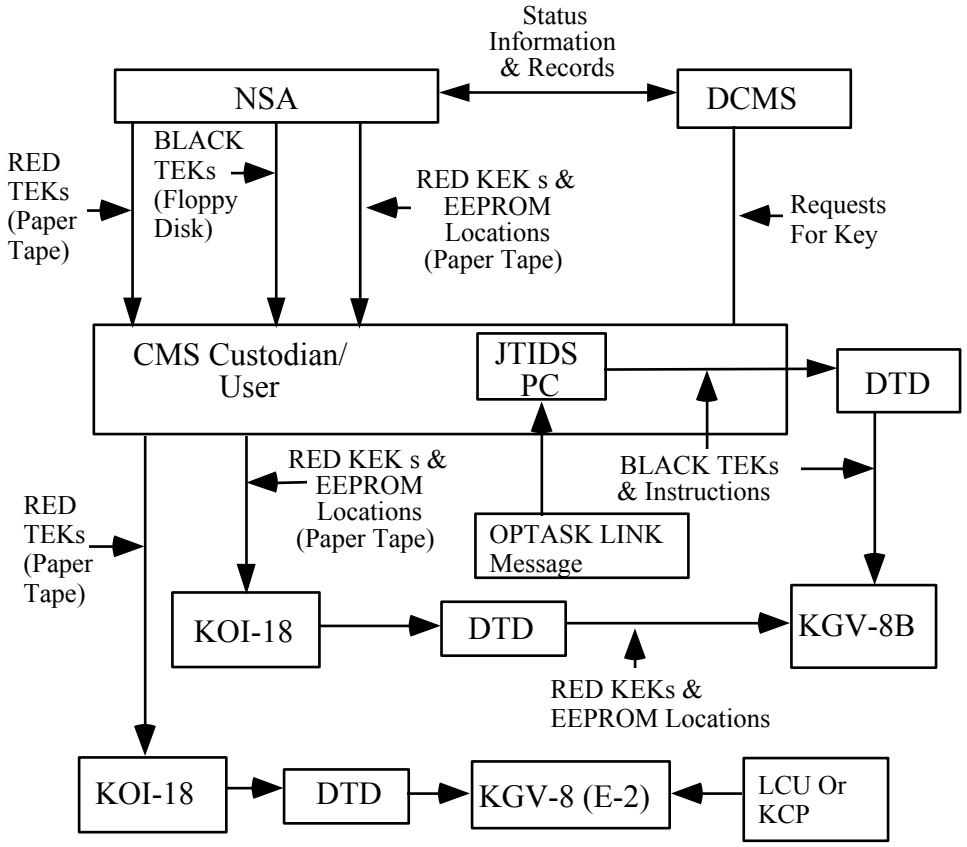


Figure 2-1 - Current Navy Link-16 Key Management Process

2.1.2 USA, USAF, and USMC Key Management. Currently, USA, USAF, and USMC Link-16 terminals use unencrypted TEKs from punched paper tape. COMSEC account managers send key requests to the USA CECOM Communications Security Logistics Activity (CSLA), USAF Cryptologic Systems Group (CPSG) Lackland AFB or the USMC Key Management counterpart, with information copies to NSA (Y132). If approved by one of these organizations, NSA generates key in punched paper form and ships it to appropriate user accounts. Local COMSEC managers submit key requests through controlling authority. Figure 2-2, depicts the current Army, Air Force, and Marine Corps Link-16 key management process.

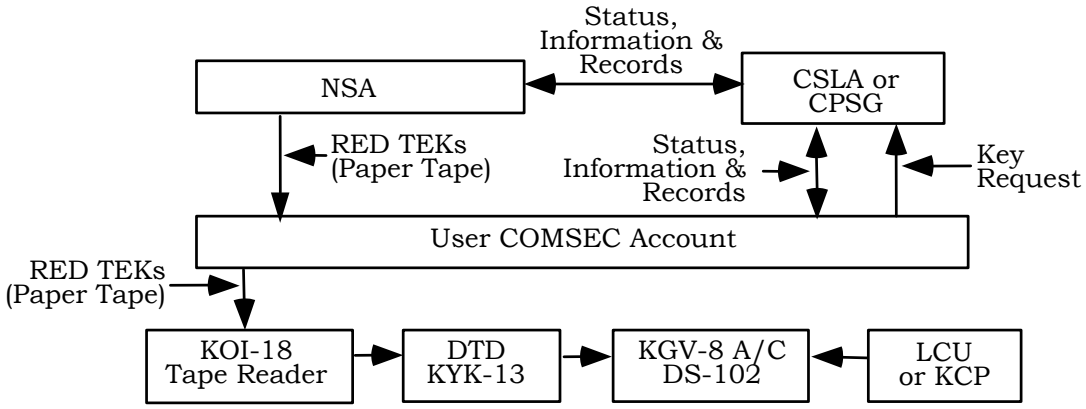


Figure 2-2 - Current Army, Air Force, and Marine Corps Link-16 Key Management Process

CHAPTER THREE
THE ELECTRONIC KEY MANAGEMENT SYSTEM (EKMS)

3.1 Description. The EKMS is a key management, COMSEC material distribution, and logistics support system consisting of interoperable Service and Defense agency key management systems. NSA established EKMS to meet multiple objectives, including supplying electronic key to COMSEC devices in a secure and timely manner and providing COMSEC managers with an automated system capable of ordering, generating, producing, distributing, storing, securing, accounting, and controlling access. Other EKMS features include automated auditing capabilities to monitor and record security-relevant events, account registration, and extensive system and operator privilege management techniques to provide flexible access control to sensitive key, data, and functions within the system. Common EKMS components and standards will facilitate interoperability and commonality among the Services.

3.2 Purpose. The ultimate goal of EKMS implementation is to reduce potential for KEYMAT exploitation by reducing human access to KEYMAT during distribution.

3.3 Background. The need for joint interoperability led to the Defense Reorganization Act of 1986, under which the Joint Chiefs of Staff (JCS) chartered the Joint Key Management Working Group (JKMWG) and a year later tasked NSA, the Defense Information Systems Agency (DISA), and the Joint Tactical Command, Control and Communications Agency (JTC3A) to develop a Key Management Goal Architecture (KMGA) in conjunction with the Combatant Commanders and Services. The JCS validated the resulting KMGA in 1988 and Minimum Required Operational Capability (MROC) 3-89 in 1989. The JCS tasked NSA, the Services, and DISA in December 1989 with implementing MROC 3-89. Difficulties in coordinating COMSEC distribution and support during joint military operations including DESERT STORM, URGENT FURY, JUST CAUSE, and ALLIED FORCE have further emphasized the need for an interoperable key management system.

3.4 Functional Description. EKMS is a four tier system.

3.4.1 TIER 0. The NSA Central Facilities (NSACF) provide a broad range of capabilities to DOD and other government agencies. These facilities comprise the EKMS Tier 0 and include the facilities located at Ft. Meade and Finksburg, Maryland. Paper-based key, allied key and non-standard electronic key are managed from the Finksburg NSACF.

3.4.1.1 NSACF Functions.

3.4.1.1.1 Seed conversion and re-key

3.4.1.1.2 Compromise recovery and management of certain key material

3.4.1.1.3 Physical and Electronic Key order processing

3.4.1.1.4 Electronic key generation and distribution

3.4.1.1.5 Conversion of existing key to EKMS (ensuring backward compatibility is retained)

3.4.1.2 Communications. The NSACF communicates with other EKMS elements through a variety of media, communication devices, and networks including direct distance protected data communication access (STU-III, STE) or dedicated link access (Omni, Omega and KG-84/KIV-7HS). Direct communication between tiers is always available. During transition to full electronic key, the 3.5-inch floppy disk and 9-track magnetic tape will be supported. Once fully operational, a TCP/IP-based message server will be the primary means of communication with the NSACF. This service will permit EKMS elements to store messages that include electronic key for later retrieval by other elements.

3.4.2 Tier 1. Prior to EKMS implementation each Service maintained a central office of record (COR) that performed basic key and COMSEC management functions, including key ordering, distribution and inventory control. In anticipation of EKMS implementation, Services began converting their key management systems to compliance with EKMS standards. A common Tier One structure that performed COR functions was implemented in 1994 to improve interoperability an commonality among the Services.

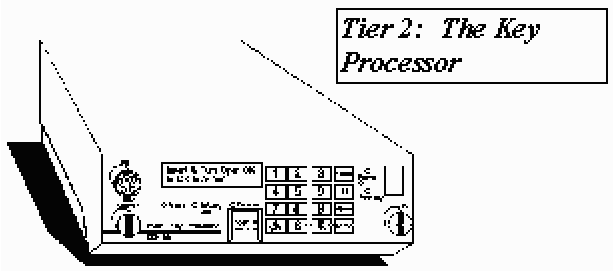
3.4.3 Tier 2. Tier 2 comprises the Base, Wing, Group, Station or Activity COMSEC account and consists of a Service or agency supplied Local COMSEC Management Device (LMD) and an NSA-supplied Key Processor (KP). The LMD is a Service or agency supplied commercial off-the-shelf (COTS) personal computer (PC). NSA-supplied Local COMSEC Management Software (LCMS) was developed to replace Service-unique automated software. LCMS is the cryptographic engine providing COMSEC Custodians and Managers the capability to electronically generate local COMSEC Key, order COMSEC material, distribute, inventory and destroy KEYMAT, and perform other COMSEC management functions. User Application Software (UAS) is being developed to provide key management for newer COMSEC equipment and weapon systems and will serve as the operator interface for LCMS.

3.4.3.1 Software. LCMS provides the interface between the LMD and the Key Processor (KP) and tools for COMSEC management. LCMS replaces the Automated Navy COMSEC Reporting System (ANCRS) and the COMSEC

Automated Reporting System (CARS) at the account level. Specialized application programs have been developed by several departments and agencies that overlay the LCMS software and provide tailored Human Machine Interface.

3.4.3.2 Platform. The LMD operates the Santa Cruz Operations (SCO 5.0) operating system and hosts LCMS. When the LMD and KP are used together, the account custodian/manager is able to order and account for all forms of COMSEC key material, store key in encrypted form, perform key generation and automatic key distribution, perform COMSEC material accounting functions, and communicate directly with other EKMS elements.

3.4.3.3 Key Processor. The KP performs cryptographic functions, including encryption and decryption, key generation, and electronic signature operations. The KP is capable of secure field generation of traditional key. Locally generated key can be employed in CRYPTONET communications, TSEC applications, point-to-point circuits, and virtually anywhere that paper-based keys are used today. Electronic keys can be downloaded directly to a KYK-13, KYX-15, or the AN/CYZ-10 DTD for further transfer or fill to the ECU.



3.4.4 Tier 3. The AN/CYZ-10 Data Transfer Device (DTD) is an NSA-developed, portable hand held device capable of securely receiving, storing, and transferring data between compatible cryptographic and communications equipment. It is capable of storing 1,000 keys, maintains an automatic internal audit trail of all security-relevant events that can be uploaded to the LMD/KP, encrypts key for storage, and is programmable. It replaces two members of family of common fill devices (CFDs), the KYK-13 and KYX-15. The DTD is capable of keying multiple information systems security (INFOSEC) devices and is compatible with such COMSEC equipment as Single Channel Ground and Airborne Radio System (SINCGARS) radios, VINSON, KG-84, and others that are keyed by CFDs. The DTD is designed to be fully compatible with future INFOSEC equipment meeting DS-101 and benign fill standards.

3.5 EKMS Key Distribution. Figure 2-1 depicts the EKMS distribution process. Paper tape key distribution will be available to users that do not have electronic distribution capability. The connection between Tier 2 and Tier 3 can be remote using various secure communication systems. Key may be loaded into the DTD directly by connecting the DTD to the LMD or KP; remotely by loading key into a local DTD and then transferring the keys and data base to another DTD via secure communication connection to a remote site; and

remotely by loading key into a local DTD and then sending the keys to a remote site via the KW-46 where the key is collected in a remote DTD at the user site.

3.6 EKMS Key Request Process. Figure 2-2 depicts the EKMS key request process. Required key must be requested by the COMSEC account supporting each Link-16 user. The request to obtain a TEK must be made to the appropriate controlling authority. Much of the TEK will be generated at Tier 0 due to the requirement for some paper key output and need to distribute key to allies. TEK for US ONLY exercises may be generated at Tier 1. ECU Encrypted Key is encrypted at Tier 2 using locally available ECU KEK through a compatible encryption process and testable through the decryption process in the KGV-8B and CDH in DS-101 mode. TEK KEKs may be generated at Tier 1 or 2 facilities. ECU Encrypted Key and ECU KEK distribution and issue is managed by the appropriate Tier 2 facility. OTAR KEK may be obtained through EKMS or through the process outlined in Appendix D of Enclosure A. (Tier 2 facilities are not capable of encrypting any keys using the OTAR KEK. This can only be done by a KOK-13.)

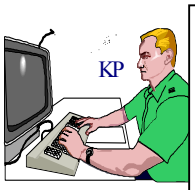
EKMS Key Distribution

Tier 0 (NSA Central Facility)
- Process Tier One Requests
- Physical Key Production
- Electronic Key Production

Defense Courier Service
- Distribute Special Ops Keys to Local Manager

Tier 1 (Service Production Facility)
- Process User Requests
- Electronic Key Production
- Distribute Keys to Local Manager (Monthly)

Tier 2 (Local Account Holder)
- Submit Key Requests as Required
- Distribute Keys to Users (Monthly)
- Comply with Controlling Authority Guidance



Tier 2 Workstation

Tier 2 (Local Account Holder)
- Submit Key Requests as Required Through Controlling Authority
- Distribute Keys to Users (Monthly)
- Comply with Controlling Authority Guidance

Tier 3 (User)
- Submit Key Requests as Required
- Load Daily Keys

Figure 3-1 - EKMS Key Distribution Process

EKMS Key Request

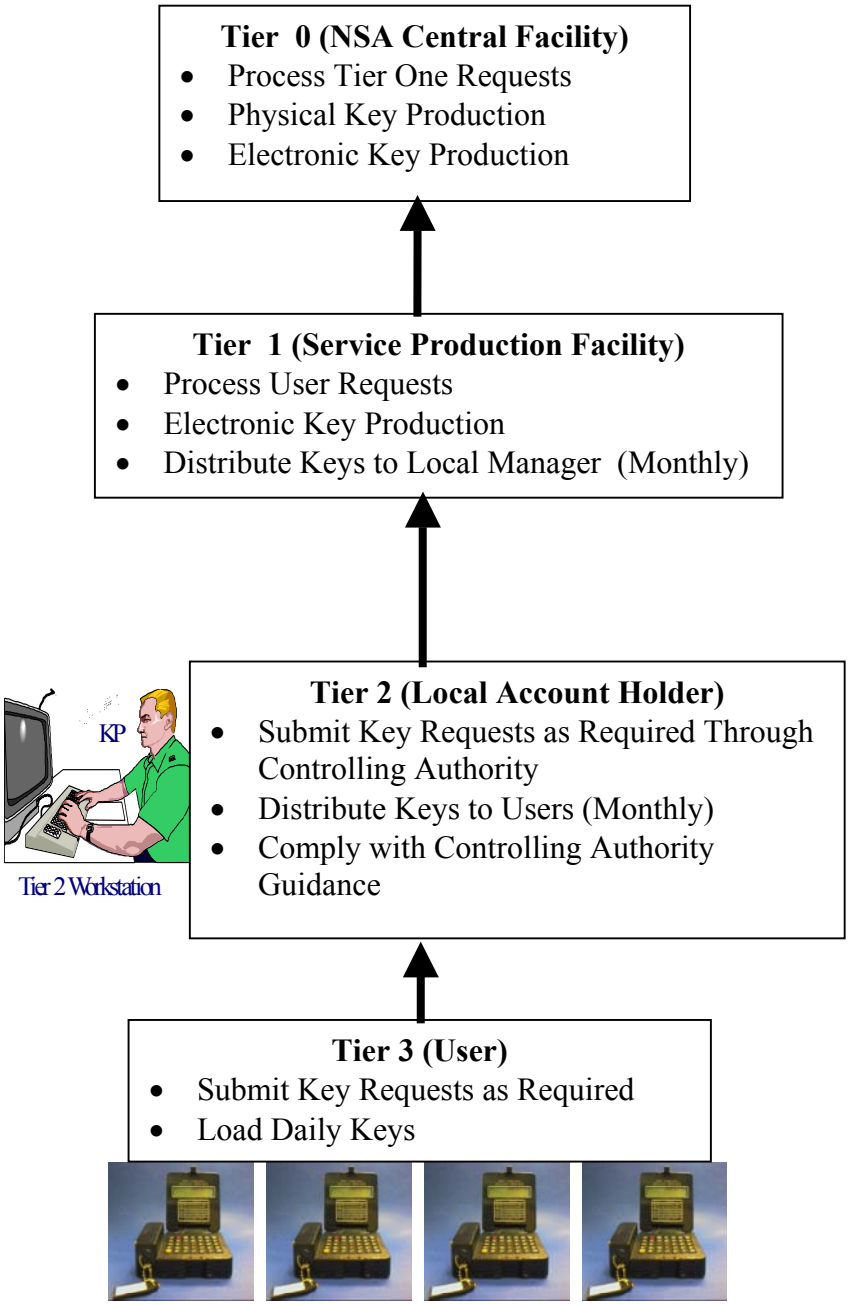


Figure 3-2 - EKMS Key Request Process

CHAPTER FOUR

EKMS KEY ORDERING PARAMETERS

4.1 Parameters. This section describes typical parameters for ordering operational key.

4.1.1 Equipment Type: Although Link-16 uses a variety of secure data units based on the CTIC cryptographic engine, EKMS only recognizes the KGV-8B and the KGV-8. Since both these devices use the same TEK type, KGV-8 has been established as the standard equipment type for ordering key. Equipment differences are selected in the KDSU or the AN/CYZ-10 CT3 software or downloaded from the DMD or ACES software into the CT3.

4.1.2 Desired Order Type: Cues EKMS to create the short title.

4.1.3 EKMS ID: Only Tier 0 can meet the requirements for generating Allied and Paper key. Therefore the EKMS ID for key generation will normally be 880091 (NSACF). If key is generated locally or by a Tier 1 entity, the appropriate EKMS ID shall be used.

4.1.4 Key Use: The only key of interest for the Joint community is the TEK. OTAR KEK, TrKEK and ECU KEK are generated by the Service or locally are not discussed here.

4.1.5 Key Purpose: Typically, this field will be operational. Other types of key (Training, Test or Maintenance) may be ordered as needed by using the parameters of this appendix.

4.1.6 Handling Restrictions: Keys are to be handled in accordance with EKMS doctrine.

4.1.7 Net Size: Cryptographic nets should be as small as operationally practical. Since net size is a required field, the number 40 is used as a place holder and is a typical operational net size.

4.1.8 Cryptoperiod: Link-16 KEYMAT for a daily key has a cryptographic period beginning exactly one minute before 0001 Universal Coordinated Time (UTC) and ending exactly one minute after 2359 UTC.

4.1.9 Segments/Edition: Daily keys are designed around the concept that segment numbers and day of the month are the same. 31 segments per edition are used to reflect this correspondence.

4.1.10 ALC: Since the operational key is reportable to COR, the ALC number is AL6. Locally accountable Training, Test, Maintenance keys are designated AL7.

4.1.11 Classification: Any key used for Link-16 operations must be SECRET. Maintenance Keys may be UNCLASSIFIED For Official Use Only.

4.1.12 Supersession Rate: Link-16 keys are subject to monthly supersession.

4.1.13 Distribution Control: An entry of "IMPLICIT" indicates the key may be copied in accordance with the directions of the controlling authority. The controlling authority must add any new accounts to the distribution profile (paragraph 1.20) to ensure the account's Reserve On Board (ROB) is adequately supported by the Tier 0 key generating account. For non-operational keys with no standing order, copies may be adequate.

4.1.14 Auth ID: [List all Controlling Authorities]. This would be the Combatant Command or JCMO ID for operational key. Non-operational key may specify a different Controlling Authority.

4.1.15 Release: [Restrictions on release]. For example, NOFORN, US/CAN/UK Only.

4.1.16 In-place-date: [The date the key should be at the destination]. Date Key should be ready for use.

4.1.17 Effective date: [Date the first key segment is effective]. No entry is currently required. The Controlling Authority can establish this at a later time.

4.1.18 Standing Order: Indicates whether the key will be produced on a continuing basis to meet ROB requirement of all of the receiving accounts.

4.1.19 Edition Info. Number of editions to be generated at one time. One is generally adequate. The maximum ROB of all the accounts to receive the key will dictate the actual number of editions produced. If there is no standing order for the key, the ordering agent must determine the number of editions to be generated as a one time production.

4.1.20 Distribution Profile: [List intended recipient(s) EKMS IDs]. At least one account must be provided. The controlling authority may add additional accounts as needed.

4.1.21 [NATIONALITY]: This field indicates whether the key is US or ALLIED. Although NATIONALITY is included here as a placeholder, the title of this field is currently undetermined.

4.2 Typical Parameters Examples.

4.2.1 Equipment type: KGV-8

4.2.2 Desired Order Type: Assign

4.2.3 EKMS ID: 880091 (EKMS ID of the Generating Element; Tier 0)

4.2.4 Key Use: TEK

4.2.5 Key Purpose: Operational

4.2.6 Handling Restrictions: No restrictions

4.2.7 Net Size: 40

4.2.8 Cryptoperiod: Daily

4.2.9 Segments/Edition: 31

4.2.10 ALC: AL 6

4.2.11 Classification: SECRET

4.2.12 Supersession Rate: Monthly

4.2.13 Distribution Control: Implicit

4.2.14 Auth ID: (Combatant Command or JCMO ID)

4.2.15 Release: (NOFORN, US/CAN/UK, US ONLY)

4.2.16 In-place-date: (Date key required to be in place at destination; when ordering Joint Operational Key, date must match DCS delivery date.)

	EUCOM	**PACOM**	**CENTCOM**	**JFCOM**	**SOUTHCOM**
Worldwide Emergency	Note 1	Note 1	Note 1	Note 1	Note 1
Joint Theater	Note 2	Note 3	Note 4	Note 5	Note 6
Allied	Note 7	Note 8	Note 9	Note 10	Note 11

Note 1: This Allied Key is to be ordered by the Controlling Authority designated by JCMO
Note 2: These US Keys are to be ordered by the Controlling Authority designated by EUCOM
Note 3: These US Keys are to be ordered by the Controlling Authority designated by PACOM
Note 4: These US Keys are to be ordered by the Controlling Authority designated by CENTCOM
Note 5: These US Keys are to be ordered by the Controlling Authority designated by JFCOM
Note 6: These US Keys are to be ordered by the Controlling Authority designated by SOUTHCOM
Note 7: These Allied Keys are to be ordered by the Controlling Authority designated by EUCOM
Note 8: These Allied Keys are to be ordered by the Controlling Authority designated by PACOM
Note 9: These Allied Keys are to be ordered by the Controlling Authority designated by CENTCOM
Note 10: These Allied Keys are to be ordered by the Controlling Authority designated by JFCOM
Note 11: These Allied Keys are to be ordered by the Controlling Authority designated by SOUTHCOM

Table 4-1 - Operational Link-16 Key Allocation

4.2.17 Effective date: (Date First Key Segment is Effective)

4.2.18 Standing Order: Y

4.2.19 Edition Info: 1

4.2.20 Distribution Profile: (Combatant Command or JCMO ID)

4.2.21 US or ALLIED depending on part of table.

4.3 Joint Operational Keys. Short titles for the key described in this matrix are not currently available; they will be provided in future revisions as they are developed. Controlling Authority (CA) responsibilities are described in NSTISSI 4006 “Controlling Authorities of COMSEC Material.”

CHAPTER FIVE

OVER THE AIR REKEY MANAGEMENT

5.1 Description. OTAR is the re-keying of remote sites via the Link-16 communication system. Although the Link-16 system does not have Over The Air Transfer (OTAT) capability since key are not extractable, it has the capability to re-key remote Link-16 equipment. The basic requirement for OTAR is the installation of a OTAR KEK in the Link-16 equipment and transmission of J31.0 and J31.1 messages to the terminal. J31.1 contains the re-key phrase and J31.0 contains supporting data for re-key.

5.2 Purpose. OTAR requirements include rapid compromise recovery, enforcing need to know data distribution, extending the number of CRYPTONETs that can be serviced, reducing exposure of critical data, and re-keying Link-16 units that are difficult to physically access. OTAR is not a preferred standard operating procedure due to the requirements for unique key at each receiving terminal. Since OTAR KEK is not retained during power down, OTAR cannot support recovery from a power interrupt.

5.3 Required Elements.

5.3.1 TSEC/KOK-13. The KOK-13 is a National Security Agency (NSA) developed cryptographic peripheral used to support local key generation and OTAR and may be used to generate OTAR KEK. KOK-13 control is performed over an IEEE-488 interface by the NCP. It requires Key Production Key (KPK) to deterministically generate OTAR KEKs and TEKs. The KOK-13 “seed” keys are accountable within the EKMS system and currently distributed as paper keys loaded with the KOI-18.

5.3.2 System Controller (SC). Normally embedded in or interfaced to the Link-16 host combat system, the SC maintains a record of station identification numbers and their unique OTAR KEKs, and maintains a record of which CVLL is associated with which memory location. The SC also tracks which keys are currently installed in each Link-16 terminal and which have received a re-key command for a specified time. Finally, the SC provides synchronization information for use by the KOK-13. Most SC functions are directed by a human operator who is responsible for knowing what keys to send and to whom. The SC must also have the capability to send a special non communicating key to each location to recover from compromise.

5.3.3 OTAR KEK. OTAR KEK must be loaded in the receiving Link-16 terminal SDU RAM location 5, and the terminal must be set to expect OTAR messages. OTAR KEK has a monthly crypto period and is unique for each terminal.

5.3.4 Re-key Messages. The J31.1 provides the terminal re-key phrase and the J31.0 provides synchronization and other supporting OTAR information.

5.4 Procedures.

5.4.1 Generate OTAR KEK. OTAR KEK may be generated by the KOK-13 (locally), EKMS or NSA. Each recipient Link-16 terminal is required to have a unique OTAR KEK to perform OTAR, although NSA may waive this requirement under special circumstances. The SC directs the KOK-13 to encrypt the TEKs and create the re-key phrase. The KOK-13 is instructed to send the re-key phrase back to the SC which then determines the time and properly inserts the re-key phrase into J31.0 and J31.1 messages.

5.4.2 Load OTAR KEK. EKMS-generated OTAR KEKs must be loaded into the KOK-13 to create the re-key phrases. KOK-13-generated OTAR KEKs are retained by the KOK-13 and issued to a DTD to be loaded into the appropriate Link-16 SDUs. The association between each terminal's unique ID and unique OTAR KEK is established and recorded by in the SC.

5.4.3 Prepare the Receiving Terminal. Each recipient Link-16 terminal must be initialized with the OTAR activation bit set to ON.

5.4.4 Transmit the Re-Key Instructions. J31.1 and J31.0 messages are transmitted from a host combat system equipped with SC functionality. For the case where a KOK-13 is being used, transmitted TEKs must be either produced by the KOK-13 or have been received via the fill port.

5.4.5 Receive the Re-Key Instructions. When the terminal receives the J31.0 and J31.1 messages addressed to it's unique ID, it acknowledges receipt and extracts the time at which the OTAR is to be accomplished. At the specified time, the terminal extracts the re-key phrase from the J31.1 message and the synchronization bits from J31.0 and transfers the key to the appropriate SDU RAM location. The SDU CVLL is updated to a new memory table from the data in the J31.0 message, and the terminal transmits a HAVCO message to indicate a successful re-key (CANTPRO is transmitted if the re-key fails for any reason). Note that since the Link-16 SDU will not change the key in any cryptovariable location until it has successfully decrypted a received re-key phrase, caution should be exercised to ensure terminals have received re-key phrases before a network reconfiguration is initiated. Failure to verify successful re-key could result in exclusion of the affected terminal from the reconfigured network.

5.5 Other Considerations.

5.5.1 TEK Extraction. TEKs that are accounted for by the EKMS and have been issued to a KOK-13 may not be extracted from the KOK-13 into a fill device.

5.5.2 TEK Redistribution. KOK-13-generated TEKs may be issued to a Tier 3 fill device for further distribution.

5.5.3 OTAR KEK Redistribution. KOK-13-generated OTAR KEKs may be issued to a Tier 3 fill device for further distribution.

5.5.5 OTAR KEK Locations. If OTAR use is anticipated, the number of short titles in continuous use that may be loaded at one time into a Link-16 SDU is reduced from four to three. Location 5 is used for the OTAR KEK. Location 4 is not used or is used as a scratch pad. Technically, the locations 0, 1, 2, 3, 6, and 7 could all be used independently but would require complex coordination to ensure participating units transition together at cryptographic period rollover.

5.5.6 Key Protection Key. The KPK needs greater protection than the other keys. In many cases the KPKs are classified as TOP SECRET CRYPTO and must be handled according to doctrine for TOP SECRET keys.

5.5.7 KOK-13 Transfer. TEKs provided or accounted for by the EKMS system are allowed to be issued to a KOK-13 for encryption and OTAR distribution. CT3 will be capable of issuing standard 128 bit key to the KOK-13.

5.5.8 KOK-13-Generated OTAR KEK. Although the KOK-13 may be used to generate OTAR KEK, this function should only be used in highly localized networks where multi-platform coordination is not required. EKMS should be used to generate OTAR KEK in all other circumstances.

5.5.9 Terminal Loading. Note that since each Link-16 terminal can hold only one key for future use at a time, the SC operator should not allow keys to be sent to a terminal if a key is already in memory waiting to be loaded.

5.5.10 KOK-13 Key Redistribution. Although keys produced by the KOK-13 can be used in Link-16 equipment for data encryption, the KOK-13 key should not be distributed through EKMS since it is not accountable for these keys. Tier 3 fill devices may be used to received key from the KOK-13 and fill equipment (the CT3 is designed to do this).

5.5.11 KOK-13 as a Key Storage Device. The KOK-13 shall not be used as a key depository for EKMS accountable keys. EKMS accountable keys issued to the KOK-13 are for encryption and OTAR distribution only.

(INTENTIONALLY BLANK)

CHAPTER SIX

JOINT KEY MANAGEMENT PLANNING PROCEDURES

6.1 Introduction. This chapter establishes key management responsibilities for various DoD entities.

6.2 Responsibilities.

6.2.1 Combatant Commanders.

6.2.1.1 Provide network design criteria to their Service network design facilities or JNDL to include COMSEC key structure.

6.2.1.2 Prepare and distribute OPTASK LINK message preparation guidance and specific key management instructions.

6.2.1.3 Notify controlling authorities of joint theater key requirements.

6.2.1.4 Implement standing orders and/or dynamic ordering procedures to support anticipated robust network structures.

6.2.1.5 Order short titles for Joint and combined in-theater requirements.

6.2.2 Network Design Facilities (NDF). Service NDFs develop networks for operations and training. CRYPTONETs must only include the participants that have a need to see data protected by the network. Network design should include Crypto Period Designator (CPD) assignments to allow rollover in a common direction.

6.2.3 EKMS Managers/CMS Custodians.

6.2.3.1 Normal Functions. Each Service has instructions concerning the EKMS Manager/CMS Custodian duties including the requirement to maintain a COMSEC inventory and Reserve on Board (ROB) adequate to support the command operational mission. Each Service is responsible for ordering short titles for intra-Service operations and testing.

6.2.3.2 EKMS Support. EKMS levies additional responsibilities on the EKMS Manger/CMS Custodian. In addition to the EKMS functions, there are Service specific UAS programs on the Tier 2 Local Management Device (LMD) used to support the CT3 system on the DTD. The EKMS Manager/CMS Custodian will need to operate the KDSU to support the Link-16 system. In some cases the EKMS Manager/CMS Custodian will be responsible for loading all platform and equipment data as well as loading the keys into the DTD. The KDSU on the Local Management Device/Key Processor (LMD/KP) will support Link-16 operations and many other cryptographic material by providing the EKMS Manager/CMS Custodian with a method of identifying and creating all the management information required by the DTD. The KDSU is capable of

requesting key and key encryption with a 256 bit ECU KEK and providing that information to a DMD, or DTD with CT3. It is also capable of requesting key and encrypting in a specified DTD TrKEK for key transfer when the ECU must receive unencrypted key. The KGV-8A, KGV-8B and the CDH in DS-102 mode is the Link-16 crypto being used. If the user has a workstation and software, the user may provide all data on a floppy disk or on paper sheet. In that case, the EKMS Manager/CMS Custodian need only assist in loading the DTD or ECU KEKs and operate KDSU on the LMD/KP to provide the data and encrypted keys on a floppy or down load this information into the DTD. The user on a work station or DMD has the responsibility of insuring the correct assignments of the keys to the memory locations.

6.2.3.3 Audit Log Maintenance. The local commander is responsible for implementing the procedures and doctrine specified for the DTD as developed by the various Services. The EKMS Manager/CMS Custodian is responsible for ensuring proper procedures are carried out regarding uploading, viewing and resetting of the DTD audit log. Additionally, the EKMS Manager/CMS Custodian is responsible for instructing the user in the user's responsibilities.

6.2.4 Users.

6.2.4.1 Loading Key. The user is responsible for loading the correct keys for the mission into the SDU. The DTD, running CT3, will assist the user in the selection of the correct segments for key loading.

6.2.4.2 Zeroizing Equipment. The SDU will zeroize TEK upon removal of power. Link-16 terminal operators must zeroize the SDU if the unit is likely to fall into enemy hands. Some aircraft provide a switch that will zeroize all equipment including Link-16, while in some systems the operator of the host system must send initiate command to zeroize the Link-16 equipment. The DTD user application software can also be used to zeroize the TEK keys and is the only way to zeroize the ECU KEK keys. During normal operation, the ECU KEKs need be zeroized only if the SDU is to be stored for a period of greater than a month or is to be shipped through commercial shipping.

6.2.4.3 Monitoring Alarms. The SDU alarm sensors monitor internal operations and perform self-tests on the alarm circuitry. Alarm conditions can be caused by loss of power sources, invalid key transfers to the SDU, time slot number errors, and physical parts within the SDU. If an alarm condition occurs, it is reported to the host terminal. The SDU then performs a series of internal checks and attempts to restore the keys in use. If the internal tests failures persist, the SDU will not operate. It is the user responsibility, upon observing an alarm condition, to evaluate the condition, determine what action is necessary to ensure security of the communication data, and take corrective

action where appropriate. SDUs for which alarms can not be removed, should be evaluated for repair. The most common problems encountered are not caused by the SDU, but the terminal battery. Proper terminal battery care will minimize the occurrence of SDU alarms.

6.2.4.4 Maintain Audit log. Service instructions establish requirements and procedures for audit log maintenance. At their discretion, local commanders may provide additional guidance to the EKMS manager. Users are responsible for complying with all applicable guidance.

6.2.4.5 Prepare Data for the DTD. The CT3 UAS software in the DTD requires that platform and equipment data be loaded into the DTD in addition to the key. The user will be required to either manually enter this platform and equipment data, or retrieve the data from a workstation. The KDSU can perform this function, but KDSU operators may not be familiar with equipment loading procedures. An operator can create the platform and equipment information by using the ACES system or the DMD. If the KDSU provides the encrypted key to the DMD it can also assign key to the appropriate ECU. The ACES system deals with unencrypted key only can down load the platform, equipment, and assignment data, but the DTD must receive the unencrypted key from the KP in key needed mode.

6.2.4.6 Monitor Cryptographic Material Access. Access control for KEYMAT and COMSEC equipment is defined in the applicable COMSEC and EKMS doctrine for each Service. When the SDU has a KEK installed, the equipment is handled as CCI containing COMSEC data classified to the level of the KEK. NSA has specific restrictions on the SDU with a KEK loaded when not in use and is stored for a month or more or is to be transported to another location. Every effort should be made to zeroize KEKs prior to storage or shipment. If this is not possible, the equipment is to be treated as an item at the classification level of the KEK. Since KEK cannot be extracted, however, it shall not to be marked "CRYPTO." Link-16 terminals are considered high value items. Protection afforded to the Link-16 terminal is adequate for the SDU that is associated with it. No special clearance is required to observe filling of any Link-16 SDU by an electronic fill device. Access to the DTD, which is also a CCI device, is covered in each Service EKMS or COMSEC doctrine. Viewing of the DTD, or DTD fill process, by personnel without COMSEC training or user status is permitted, except when loading key marked "CRYPTO" in paper form.

6.2.4.7 Monitor Link-16 System Access. Since the keys are not extractable from the SDU, personnel possessing clearances to the level of the traffic transmitted or received are permitted access to the areas operating a Link-16 terminal. CMS user status is not require unless key is exposed. Anyone may observe the Link-16 equipment with or without the SDU being visible. Link-16

SDUs for all operational units are Controlled Cryptographic Item (CCI), and should be handled in accordance with current CCI doctrine. The MIDS, Fighter Data Link (FDL), the Class II PIP terminals are considered CCI. Special handling doctrine should be utilized to accommodate the large equipment.

6.2.4.8 Accounting. Link-16 Key accounting is accomplished via the EKMS accounting system, and will comply with service COMSEC doctrine and EKMS UAS capabilities.

6.3 Key Generation.

6.3.1 EKMS TEK. Joint TEK will normally be generated at EKMS Tier 0 or Tier 1. TEK may be generated at the Tier 2 level in special circumstances. Each Service may have the keys used for their operations generated at EKMS Tier 0, 1 or 2 levels.

6.3.2 EKMS ECU KEK. When ECU KEKs are required, they should be generated at the lowest level with facilities to support distribution (normally Tier 2). Common KEKs are required where there is shared DTD usage, even if it is only for emergency backup. For example, all elements of a Navy Battle Group will have the same ECU KEKs, allowing any DTD with Link-16 ECU Encrypted Keys to load any Link-16 SDU.

6.3.3 EKMS DTD KEK. DTD KEKs are part of the EKMS concept of operations. There is one DTD KEK per COMSEC account, generated in accordance with the EKMS.

Link-16 Key Type	**Users**	**Purpose**
TSEC	All Users	Network Synchronization
MSEC[1]	All Users	Coalition Tactical Data
MSEC	All US Forces Users	US Force Tactical Data
MSEC	Specified US Forces Users	US Air-to-Air
MSEC	Specified Coalition Users	Coalition Air-to-Air
TSEC or MSEC	All Users	Emergency Contingency

[1] One short title may be used to satisfy common TSEC and MSEC requirements.

Table 6-1 - Nominal Combined Force COMSEC Requirements

6.4 Key Distribution. Table 6-1 details the nominal operational requirements for key to support a Combined Task Force. Short titles listed are only

examples. As a minimum, two coalition-releasable and two US-only cryptographic short titles are required. The number of short titles that may be loaded at one time is reduced from four to three if OTAR is anticipated. Contingency key is included to support emergent COMSEC interoperability requirements. Each Service is responsible for ordering short titles for intra-Service operations and testing.

6.4.1 Requesting Key. Required key must be requested by the EKMS Tier 2 COMSEC account supporting the user from the EKMS Tier 0 or Tier 1 facilities. To minimize risk of compromise and vulnerability to exploitation, ECU Encrypted Keys, both TEK and KEK shall be used wherever feasible.

6.4.2 Receiving Key.

6.4.2.1 ECU KEK. Tier 2 distribution points may receive ECU KEK from Tier 1 or generate KEK for distribution to their user accounts. User COMSEC accounts may receive Link-16 KEK in their Tier 2 LMD/KP directly from Tier 1 or from their serving EKMS Tier 2 distribution point for further issue to a DTD for loading into an ECU.

6.4.2.2. TEK. User COMSEC accounts may receive TEK in their Tier 2 LMD/KPs from either Tier 1 or Tier 0 or their serving EKMS Tier 2 distribution point. TEKs may be encrypted at Tier 2 using a KEK obtained from a Tier 1 facility (or a generated locally) upon request from a Tier 2 UAS (e.g., KDSU) and the resulting encrypted TEK distributed by the Tier 2 UAS to the DTD running CT3.

6.5 Key Storage.

6.5.1 SDU. All JTIDS SDUs are capable of storing eight unencrypted keys in RAM. The CDH can store 64 keys in RAM. The KGV-8B and CDH can store KEK in any of nine EEPROM locations. All keys stored in the SDU are non-extractable.

6.5.1.2 RAM Storage. In an SDU with eight or more key storage locations, the convention described in Table 6-2 will normally apply, although changes may be made according to operational requirements. The network selected for terminal initialization controls the actual locations used. Once a network has been selected (or constructed by a network design facility based on operational requirements), the locations and the use of those locations is fixed by that network. Short titles are assigned based on the usage defined in the same network.

6.5.1.1 EEPROM Storage. Although the KGV-8B and CDH are capable of storing TEK in EEPROM, the ability to later use these TEKs requires DTD capabilities for which no software currently exists. Access to these devices

would also be affected if TEKs were stored in the EEPROM. A detailed plan and formal request for authorization from NSA is required prior to use of EEPROM for TEK storage. Additionally, EKMS user application software must be modified to accommodate EEPROM TEK loading. If a Service requires this capability, an Engineering Change Proposal (ECP) must be submitted to the applicable Software Support Activity (SSA) for the requesting CT3 DTD UAS.

Storage Locations	0-1	2-3	4-5	6-7
Network defined Key Use	Normal Operational Key in Common Variable Mode or TSEC in Partitioned Variable Mode	1st MSEC	OTAR or 2nd MSEC	Allied Key or 3rd MSEC if required

Table 6-2 - Crypto Storage Location Guidance

6.5.2 LMD. The LMD only stores Encrypted keys. Unencrypted key must first be encrypted by the KP before being stored in encrypted form on the LMD hard drive.

6.5.3 AN/CYZ-10 DTD. The AN/CYZ-10 DTD can store 1,000 unencrypted TEK and their associated key tags. ECU Encrypted Keys are larger than unencrypted keys; consequently fewer encrypted keys can be stored. They can be secured by removing the Crypto Ignition Key (CIK) from the device. With its CIK removed, the AN/CYZ-10 becomes an UNCLASSIFIED controlled cryptographic item. Stored keys can be selectively deleted or zeroized. The AN/CYZ-10 DTD must be zeroized to remove all keys and downgrade the AN/CYZ-10/CIK to UNCLASSIFIED.

6.5.4 KYK-13 and KYX-15. The KYK-13 can store six unencrypted keys, and the KYX-15 can store 16 keys. Both can zeroize keys collectively or selectively.

6.6 Key loading. TEKs shall be loaded into the SDU in adjacent pair RAM storage locations. Successive key segments shall be loaded into the SDU if operation is anticipated through a cryptographic period transition. If the terminal has been turned off, both the current day and next day TEK must be reloaded. Terminals using the KGV-8B must be loaded with the all of the current and next day TEKs needed for the network configuration every time key is loaded. Currently, key loading may only be accomplished through the fill port or OTAR. MIDS development planning includes the capability to allow ECU Encrypted Key fill over the IEEE 1553 bus (or any other bus by which data is sent to the MIDS terminal). Single point keying (where several

cryptographic devices using the DS-101 protocol can be keyed at the same time over a fill bus) has been implemented in some Link-16 platforms. A bus (STATION) address is used during DS-101 key loading to direct keys to the correct terminal SDU. The management of Station Addresses for bussed SDUs is the responsibility of each Service platform Program Office (e.g., NAVAIR PMA-265 for the F/A-18). EKMS supports single point keying.

6.7 Cryptoperiods.

6.7.1 KEK. The cryptoperiod for each Link-16 KEK is one calendar month commencing at the beginning of the minute defined by 010001 UTC.

1.1.1. 6.7.2 TEK. The cryptoperiod for each Link-16 TEK is one day and, except when using time offset to operate independent networks, commences at the beginning of the minute defined by 0001 UTC.

6.7.3 CPD Initialization. Even RAM locations shall be initialized to the same CPD and the odd locations shall have the opposite CPD.

6.7.4 Cryptoperiod Extension. The Link-16 design does not permit operator initiated extension of the key cryptoperiod. The cryptographic period for Link-16 is 24 hours, normally commencing at the beginning of the minute defined by 0001 UTC. Explicit coordination and a Joint Service agreement are required to use a seven-day crypto period and will be addressed in a separate addendum to this plan when the engineering is accomplished to use this capability.

6.8 Compromise Procedures. COMSEC incidents are reported in accordance with National Security Telecommunications and Information Systems Instruction (NSTISSI) 4003, "Reporting and Evaluating COMSEC Incidents," and its Service implementers.

6.8.1 Unencrypted TEK Compromise. If an unencrypted TEK is compromised, the encrypted copy of the same TEK is also compromised. Compromise recovery strategy is to supersede the compromised TEK edition and use the next sequential TEK edition. If TEK recovery requires a KEK change, the appropriate KEK segment used to encrypt/decrypt the encrypted TEK must be superseded, and the next KEK segment shall be used.

6.8.2 Encrypted Key Compromise. Loss of a encrypted TEK or encrypted KEK is not a compromise. A physically lost key shall be replaced with an identical key.

6.8.3 Unencrypted KEK Compromise. If a unencrypted KEK is compromised, all keys encrypted with that KEK are also compromised. Recovery procedure for a compromised KEK segment is to supersede that segment and all editions of keys encrypted by that KEK and implement the next KEK segment and corresponding key edition encrypted by that KEK. The recovery procedure for a

compromised KEK edition is to supersede all key editions encrypted by that KEK and implement the next KEK edition and corresponding key editions encrypted by that KEK. If no uncompromised KEK editions and associated encrypted key are available, new KEKs and TEKs must be requested from the EKMS Tier 1 or Tier 2 facility.

6.8 OPTASK LINK. The formatted message for Operational Tasking Data Links (OPTASK LINK) defined by MIL-STD-6040 is used to provide detailed instructions regarding the tactical data link operations. The OPTASK LINK contains COMSEC key identification, link operating frequencies, channelization, and initialization plans. The OPTASK LINK is used by terminal platforms to plan and conduct joint tactical communications for a designated period. Included in the Link-16 portion are instructions for the preparation and loading of the COMSEC keys required for link operation.

6.8.1 PERIOD Set. Each OPTASK LINK message contains a line that indicates network start times, which specifies the effective period of operation for the tactical data links. If the effective period of Link-16 operations differs from the general effective period of the OPTASK LINK message a separate PERIOD set is included in the Link-16 section.

6.8.2 JCRYPDAT Set. The cryptographic data (CRYPDAT) set section of the OPTASK LINK message specifies unique COMSEC requirements. It relates COMSEC short titles to Crypto Variable Logic Label (CVLL) CRYPTONET numbers and indicates into which SDU storage location each short title should be loaded.

6.8.3 JUDATA Set. The Unit Data Set identifies the JU (JTIDS Unit) number of specific user platforms (e.g., ship, aircraft) as well as message data requiring unique parameters.

6.8.4 JSDULOC Set. The SDU location (JSDULOC) set is a subset of the JUDATA set in the OPTASK message for platforms that are exceptions to the COMSEC requirements specified by the Link-16 CRYPDAT set. The SDULOC set indicates the CVLL number and the SDU locations for the specified Link-16 platform. The OPTASK LINK message will not be modified to accommodate 64 locations of the MIDS LVT-(2) terminal. If higher locations are used the terminal will appear as having only 8 locations.

6.8.5 AMPN/NARR Set. An amplification or narrative set is included after the CRYPDAT set or JSDULOC sets to indicate the current cryptoperiod designator (CCPD), advising Link-16 users whether to load keys into even or odd SDU locations. The CCPD is 0 on January 1, 1985, and alternates between 0 and 1 each day thereafter (see Table 1-4).

ENCLOSURE B

LINK-16 KEY MANAGEMENT CONTACT LIST

Agency	Message Address	Web Address
SPAWARSYSCEN D4524 53560 Hull St San Diego, CA 92152-5001	SPAWARSYSCEN SAN DIEGO CA//D4524//	
Director National Security Agency 9800 Savage Rd Ft. George G. Meade, MD 20755-6000	DIRNSA FT GEORGE G MEADE MD//V322/V34/V51//	
HQ ESC/DIWK-1 (AFEKMS) 240 Hall Blvd Ste 102 San Antonio, TX 78243-7057		
Joint COMSEC Management Office 8532 Marina Bay Dr MacDill AFB, FL 33611	JOINT COMSEC MANAGEMENT OFFICE MACDILL AFB FL	
Director Communications Material Systems Nebraska Avenue Complex 4255 Mount Vernon Drive Suite 17337 Washington, DC 20393-5453	DCMS WASHINGTON DE// 34//	
Joint Interoperability Test Command Ft. Huachuca, AZ 85635		

(INTENTIONALLY BLANK)

GLOSSARY

This glossary contains acronyms and definitions found in this document or likely to be encountered in Link-16 communications security management.

PART I—ABBREVIATIONS AND ACRONYMS

C2	Command and Control
CA	Controlling Authority
C2P	Command and Control Processor
CCI	Controlled Cryptographic Item
CCPD	Current Cryptoperiod Designator
CDH	COMSEC/TSEC Integrated Circuit (CTIC) Hybrid
CFD	Common Fill Device
CFDI	Common Fill Device Interface
CIK	Crypto-ignition Key
CMS	COMSEC Material System
COMSEC	Communications Security
COR	Central Office of Record
CPD	Cryptoperiod Designator
CPSG	Cryptologic Systems Group (Air Force)
CSP	Common Signal Processor
CT3	Common Tier 3
CTIC	COMSEC/TSEC Integrated Circuit
CVLL	Crypto Variable Logic Label
CVM	Common Variable Mode
DCMS	Director, COMSEC Material Systems (Navy)
DIRNSA	Director, National Security Agency
DMD	Data Management Device
DTD	Data Transfer Device
ECP	Engineering Change Proposal
ECU	End Crypto Unit
EEPROM	Electronically Erasable Programmable Read Only Memory
EKMS	Electronic Key Management System
FCI	Function Control Information
FDL	Fighter Data Link
FES	Front End System
GMT	Greenwich Mean Time
IJMS	Interim JTIDS Message Specification

JCMO	Joint COMSEC Management Office
JKMP	Joint Key Management Plan
JNL	JTIDS Network Library
JTIDS	Joint Tactical Information Distribution System
JUDATA	JTIDS User Data
KCP	Keyer Control Panel
KDSU	Key Distribution Support UAS
KEK	Key Encryption Key
KP	Key Processor
KPK	Key Production Key
LCMS	Local COMSEC management Software
LCU	Load Control Unit
LMD	Local Management Device
LVT	Low Volume Terminal
MHz	Megahertz
MIDS	Multifunctional Information Distribution System
MSEC	Message Security
NDA	National Distribution Authority
nm	Nautical Mile
NPG	Network Participation Group
NSA	National Security Agency
NSACF	National Security Agency Central Facility
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
OPTASK LINK	Operational Tasking Data Links
OTAR	Over-The-Air Re-keying
OTAT	Over-The-Air Transfer
PIP	Product Improvement Program
PPLI	Precise Participant Location and Identification
PVM	Partitioned Variable Mode
RAM	Random Access Memory
ROB	Reserve On Board
RTT	Round Trip Timing
SDU	Secure Data Unit
SMP	Signal Message Processor
SSA	Software Support Activity
TAMPS	Tactical Aircraft Mission Planning System
TCU	TSEC/COMSEC Unit
TDMA	Time Division Multiple Access
TEK	Traffic Encryption Key
TSK	Transmission Security Key
UTC	Universal Coordinated Time

UAS	User Application Software
USACSLA	U.S. Army CECOM Communications Security Logistics Activity.
USMTF	United States Message Text Format

PART II--DEFINITIONS

Allied. A term used within this document to refer to operations between or key used by the US and member nations of a treaty organization (i.e., NATO), coalition or combined force.

BLACK Key. Encrypted Key.

Common Signal Processor (CSP). Product of the JTIDS Class II Terminal Embedded Crypto Card Product Improvement Program (PIP).

Common Tier Three Software. DTD software used to fill all operational crypto devices.

Common Variable Mode (CVM). Mode of operation in which the same key is used for both traffic encryption/decryption and transmission security.

Controlled Cryptographic Item (CCI). Secure telecommunications or information handling equipment, or associated cryptographic component, that is unclassified but governed by a special set of control requirements.

Controlling Authority (CA). Official responsible for directing the operation of a CRYPTONET and for managing the operational use and control of keying material assigned to the CRYPTONET. In Link-16, the official responsible for the proper security and use of a COMSEC short title.

Cryptographic Network (CRYPTONET). A collection of operational units whose data is being protected from all others by the encryption process provided from a single Crypto Key. Link-16 can operate with multiple CRYPTONETs simultaneously. Note that multiple NPGs can be operating in the same CRYPTONETs.

Cryptographic Variable Logic Label (CVLL). Tie between short titles and network design. Also tie between SDU memory locations and network design.

Current Cryptographic Period Designator (CCPD). One bit parameter used to determine what set of keys are in use on a particular day. See Table 1-4.

Data Management Device (DMD). Air Force software package that runs on a PC or Palm top that creates the management information for the CT3. It also will interface with the KOV-21 to act as a fill device. It will operate with or without the KOV-21.

Data Transfer Device (DTD) Encrypted Key. Key data that results from a key being encrypted in a TrKEK.

Data Transfer Device (DTD). Common name for AN/CYZ-10.

DS-101. EKMS standard for electronic key transfer.

DS-101 KEK. KEK used in the KGV-8 and CDH to encrypt/decrypt keys transferred via DS-101.

Electronic Key Management System Key Encryption Key (EKMS KEK). Key Encryption Key used to encrypt data for transport from one COMSEC account to another.

End Cryptographic Unit (ECU). Generic name for any crypto device. Sometimes referred to as Tier 4.

End Cryptographic Unit Encrypted Key (ECU KEK). Key data that results from a key being encrypted in an ECU KEK.

Fighter Data Link (FDL). MIDS LVT3. MIDS variant used in F-15s.

Front End System (FES). Receive only Link-16 terminal. The CDH is embedded on the TSEC/COMSEC Unit (TCU). The unit can be set from the front panel to be either DS-101 or DS-102.

Function Control Information (FCI). Data that controls what a THORNTON smart fill is to do with the information/key that is being received.

Interim Joint Tactical Information Distribution System Message Specification (IJMS). Message Standard for Class I JTIDS terminals. Still used in NATO and some Air Force E-3 Aircraft.

Interoperability Standards for Electronic Key Management Systems (ISEKMS). Replaces the previous standards: DS-100, DS-101, DS-102 and NSA 87-27 are contained.

Joint Cryptographic Data (JCRYPTDAT). Cryptographic data annotated in the OPTASK LINK message.

Joint Security Data Unit Locator (JSDULOC). OPTASK LINK Data Field.

Joint Tactical Information Distribution System (JTIDS) Network Library (JNL). Compendium of JTIDS networks, normally distributed as a single magnetic media item.

Joint Tactical Information Distribution System (JTIDS) Unit Data (JUDATA). OPTASK LINK Data Field.

Key Distribution Support User Application Software (KDSUAS). Key Distribution Support UAS - A Navy UAS to work with the LCMS in the EKMS system to provide support data and key to the CT3 on a DTD from the LMD/KP.

Key Encryption Key (KEK). Key used to encrypt or decrypt other keys for transmission or storage.

Key Processor. KOK-22A.

Key. In this context, "key" refers to the information bits that specify the generation of protection hiding bit stream which is used to hide the intelligent information transmitted through the communication system. In many of the older documents, the name Crypto Variable is used. DIRNSA has directed the Key be used instead of Crypto Variable.

Keyer Control Panel (KCP). Device used to set the memory address into which the key goes. Load Control Unit (LCU) is a KCP in a box for Navy Air Craft Ship use on flight deck. The KCP is required for DS-102 Key fill. The DS-101 key fill does not require a KCP, the memory location is set by the software in the AN/CYZ-10.

Link-16. Jam resistant line of sight tactical data and voice communication system with relative navigation capabilities.

Load Control Unit (LCU). Mechanically encapsulates a Keyer Control Panel.

Local Communications Security (COMSEC) Management Software (LCMS). Software runs on the LMD to control and utilize the KP. A basic part of Tier 2.

Local Management Device (LMD). Central element of Tier 2 account.

Megaherz (MHz). One million cycles per second.

Message Security (MSEC). Security afforded to transmitted textual data by a machine cryptographic system. Field in the Link-16 terminal that designates the isolating crypto short title to protect the message content of designated NPGs using the CVLL.

Military Standard 6016A. Document defining message formats and data elements for Link-16 messages.

Multifunctional Information Distribution System (MIDS) Low Volume Terminal (LVT). Family of Link-16 transceivers designed for integration in various airborne and air defense platforms. Current variants include the MIDS LVT(1), LVT(2) and LVT(3), also commonly referred to as the Fighter Data Link (FDL) terminal.

National Distribution Authority (NDA). National Security Agency Key Production and Distribution.

National Security Agency (NSA) 90-2A. THORNTON smart fill data standard. It is a DS-101 base standard with the special fields required for the THORNTON smart fill defined.

National Security Agency Central Facility (NSACF). Key Production Tier Zero.

Network Participation Group (NPG). A unique list of applicable Link-16 messages used to support an agreed technical function without regard to subscriber identities. This list is a means of transmitting a common set of Link-16 messages to all interested users. Frequently used NPGs include electronic warfare, command and control, network synchronization, et al.

Operational Tasking Data Links (OPTASK LINK). USMTF message that provides detailed instructions regarding tactical data link operations, including information required to establish these links.

Over-the-air Re-key (OTAR) Encrypted Key. Key data that results from a key being encrypted in an OTAR KEK, sometimes referred to as the “re-key phrase.” These Encrypted keys can only be loaded from the transmission side of the Link-16 terminal via J31.0 and J31.1 messages. They cannot be loaded through the fill port.

Over-the-air Re-Key (OTAR) Key Encryption Key (KEK). KEK used in a SDU to decrypt keys received via OTAR. Sometimes referred to as a “unique.” In EKMS OTAR KEK is referred to as KGV-8 KEK or OTAR KEK. The OTAR KEK can be loaded through the fill port.

Over-the-air Re-key (OTAR). Changing traffic encryption key or transmission security key in remote cryptographic equipment by sending new key directly to the remote cryptographic equipment of the communications path it serves. In Link-16, a special capability of the CTIC cryptographic engine that enables over the air key delivery without the need for a physical fill device.

Partitioned Variable Mode (PVM). Mode of operation in which a different message security traffic encryption key is used to secure specific compartmented data that is used for other Link-16 data and for Link-16 transmission security for traffic encryption/decryption and transmission security.

Product Improvement Program (PIP). JTIDS Class II Terminal Upgrade program.

Random Access Memory (RAM). Computer memory that provides the main internal storage available to the user for programs and data. Sometimes referred to a "volatile" memory. There are 8 memory locations in the Secure Data Unit that are volatile and used for TEKs and OTAR KEKs. The Army MIDS Variant (MIDS LVT(2)) has 64 RAM locations.

RED Key. Unencrypted key.

Re-key Phrase. See entry under OTAR Encrypted Key.

Reserve-on-board (ROB). Amount of Key required to be present at an account for future use, because the account will not be able to communicate with the account that generates the key for a period of time.

Round Trip Timing (RTT). Messages sent and received that are used to accurately assess the distance between terminals.

Secure Data Unit (SDU). Functional name for the THORNTON cryptographic equipment used in Link-16 terminals. Link-16 SDUs include the KGV-8/A/B/C in the JTIDS Class II, the E-GLD in some of the Army systems, the CDH in the CSP card and in the SMP card of MIDS.

Signal Message Processor (SMP). Processing card of the MIDS terminal that processes signals and raw messages.

Software Support Activity (SSA). Each COMSEC software package is required by DIRNSA to have an SSA established to correct problems and added new capabilities.

Tactical Aircraft Mission Planning System (TAMPS). System used to build the network to be installed in the Link-16 system. The NCS for the Army and the C2P for the ships do similar functions. TAMPS is off line, whereas C2P and NCS are on line and exercise communication functions as well.

THORNTON. Project name that refers to the KGV-8 equipment and the THORNTON embedded products.

Tier Four. This tier is generally identified with the ECUs.

Tier One. Service Production facility - this tier has large production capabilities for electronic key, but none for physical key.

Tier Three. This is the user level of the system. The user holds and uses the AN/CYZ-10 to fill Tier 4 equipment.

Tier Two. Designation of the local account holder. The LCMS running on the LMD connected to KP makes up the back bone of this tier.

Tier Zero. Central Facility at NSA. This facility is capable of doing Tier 1 functions. It also forms the bridge between USA and other countries.

Time Slot. The minimum burst of communication possible in Link-16. One or more Link-16 messages are transmitted in each Time Slot. A Time Slot is 7.8125 milliseconds in duration. 128 Time Slots are assigned each second for a total of 1536 time slots within each 12 second frame.

Traffic Encryption Key (TEK). Key used to encrypt plain text or to superencrypt previously encrypted text and/or to decrypt cipher text. Within the Link-16 system, TEK provides both transmission security (TSEC) and message security (MSEC).

Transmission Key Encryption Key (TrKEK). KEK used to decrypt keys in the AN/CYZ-10 DTD.

Transmission Security (TSEC). The component of communications security that results from all measures designed to protect transmissions from interception and exploitation by means other than cryptoanalysis. Within the context of this document, it is used to identify fields in the Link-16 terminal that tie transmission security and message security of NPGs supporting normal communication messages to the short title via the CVLL. Special NPGs may use MSEC for the message security and the TSEC for the transmission security.

Transmission Security (TSEC)/Communications Security (COMSEC) Unit (TCU). Part of the FES that is CCI and handles the interface to the CDH.

Transmission Security Key (TSK). Keying material that provides transmission security in a system. In the Link-16 system the TEK performs both the TEK and TSK functions. Although EKMS provide the selection of the TSK, there is no way to distinguish the TSK from the TEK within the Link-16 terminals. DIRNSA generally considers the TSK as a lower risk than the TEK. The Link-16 terminal will very likely use any key it is given to perform as with the TEK function. Therefore all traffic keys should be designated as TEKs and never as TSKs.

Universal Coordinated Time (UTC). A measure of time that conforms, within a close approximation, to the mean diurnal rotation of the Earth and serves as the basis of civil timekeeping. Used to establish the valid cryptographic interval for Link-16 keying material.